Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for Law	)	ET Docket No. 04-295
Enforcement Act and Broadband Access	)	
Services	)	RM-10865
	)	

Comments of VeriSign, Inc.

Anthony M. Rutkowski
Vice President for Regulatory Affairs
VeriSign Communications Services Div.
21355 Ridgetop Circle
Dulles VA 20166-6503
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

Peter Wiederspan
Director, NetDiscovery Service
4501 Intelco Loop SE
Olympia, WA 98503
Tel: +1 360.493.6220
mailto: pwiederspan@verisign.com

Michael Aisenberg
Director, Government Relations
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
Tel: +1 202.973.6611
mailto:maisenberg@verisign.com

Brian Cute
Director, Government Relations
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
tel: +1 202.973.6615
mailto:bcute@verisign.com

Filed: 14 November 2005

EXECUTIVE SUMMARY

VeriSign supports the actions taken by the Commission in the *First Order* to provide for digital forensic capabilities in the nation's communication infrastructure, and will continue to do everything possible in the marketplace through its NetDiscovery Service™ to implement the required CALEA capabilities at low-cost and minimal operational and evolutionary impact for all affected providers.

The Commission in the Notice of Proposed Rulemaking (NPRM)[1] is moving forward with the appropriate critically-important measures intended by Congress to ensure that judicially approved communications assistance to law enforcement will remain available for forensic evidentiary and investigatory purposes in Next Generation Networks that include IP-Enabled Services.

The use of the E911 VoIP scope definition seems too narrowly drawn for CALEA support purposes – as the Commission suggests itself in the NPRM in dealing with "managed" VoIP services that should be subject to CALEA. A vast array of new SIP-based VoIP offerings that do not connect to the PSTN would be placed beyond the assistance capabilities of CALEA – a result that would significantly impede law enforcement. VeriSign suggests that the scope of the CALEA requirements encompass all providers of VoIP signalling generally available to the public – for which innovative new standards are being developed by industry.

It is not apparent how the Commission could institute exemptions to the requirements without effectively giving notice to wrongdoers that to avoid the reach of law enforcement or disrupt the national communications infrastructure, they need only visit a small or rural access site, a college campus, or corporate "extranet" enabling access generally available to the public. Such a result is clearly untenable. Given the availability of highly cost-effective trusted third party CALEA compliance services from parties such as VeriSign, there are also no financial or equitable bases for such exemptions. No special class of provider should be created, given extensions of time for compliance, or otherwise treated differently, and they should be also subject to ancillary obligations to register and maintain minimally authenticated directories.

[1] *First Report and Order and Further Notice of Proposed Rulemaking in the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, RM-10865, Document 05-153, released 23 September 2005, (hereafter referred to as *First Order* and *Further Notice*).

1. For more than a decade, VeriSign has provided an array of large-scale, ultra-high availability, trusted infrastructures that enable communications, commerce and content capabilities for a broad array of network-based business and consumer services – whether it be contemporary PSTN or CMRS, SMS/MMS, Internet, Web, Internet access, traditional voice telephony, VoIP, multimedia, security, fraud management, or IP-enabled Next Generation Networks. VeriSign operates through various divisions that have offices and staff in the U.S. and worldwide. In these various capacities, it participates in scores of different forums, working collaboratively with both industry and government to find entrepreneurial-oriented solutions.

2. As part of these commercial "intelligent infrastructure" support services, VeriSign provides as a Trusted Third Party both lawfully authorized electronic surveillance (lawful interception) capability requirements to communication providers globally, and other lawful access services (i.e., subpoena processing). It also participates in or leads many of the related technology, industry, and standards activities. VeriSign is a significant interested party in this proceeding. It has been involved from the outset, and is uniquely positioned to provide perspective and expert comment in the *Further Notice*.

A. Introduction

3. The technical, operational, and enforcement measures being implemented in this proceeding provide critically important digital network forensic capabilities not only to support law enforcement needs, but also to protect the nation's public communications infrastructure. The actions are responsive - under both CALEA and Title I of the Communications Act - to fundamental changes in the national and worldwide public communications infrastructure and its use, including the statutory mandate to protect life and property.[2] The proposed requirements are necessary to deal not only with the significant rise in electronic communications based economic and personal crimes and terrorism, but also for the greater vulnerabilities of open, IP-enabled network platforms that facilitate always-on and nomadic users and providers employing a virtually endless

[2] *See* Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279; 47 U.S.C. § 151, *et seq*.

array of peripheral devices and local networks. This need is underscored by the consonance of Commission actions with similar steps being taken worldwide by regulatory authorities and law enforcement as a global response to the technology changes, increased security threats, and cybercrime.

B. Provisions of the *First Order*

4. The *First Order* carefully, albeit narrowly, instituted the steps Congress intended under CALEA, as well as what was appropriate to meet its Title I responsibilities. The *Order* also reflected the findings of the Court in the *Brand-X Decision* that underscored the importance of the Commission's unique expertise and responsibility for the national public communications infrastructure today.[3] Congress in 1994 repeatedly emphasized that CALEA was a generic requirement to assist law enforcement in obtaining needed forensic evidence that should evolve with the technology and its deployment as public services.

5. As the Commission increasingly moves away from common carrier regulatory models – which VeriSign applauds - the exercise of Title I authority is increasingly important as it puts into place needed public infrastructure capability requirements for open Next Generation Networks. This includes everything from public safety and emergency preparedness requirements to consumer protection and competitive unbundling mandates for signaling systems and services.

6. The *First Order* pragmatically focused on two critical places in the national communications infrastructure where digital forensic evidence exists - in the facilities of 1) broadband Internet access providers and 2) voice telephone service providers to the extent they were interconnected with the public telephone infrastructure. These locations represented minimal technological choke points where forensic evidence is uniquely available - not only for evidentiary purposes, but also for network management and the protection of networks. It is worth noting that other regulatory bodies throughout the world have come to similar conclusions. Indeed, the global nature of these requirements has resulted in the forensic capabilities already being implemented by vendors in

[3] *See National Cable & Telecomms. Ass'n* v. *Brand X Internet Servs.*, 125 S. Ct. 2688 (2005).

infrastructure systems at low cost with no adverse impact on performance or evolution of the technology.

7. VeriSign believes, however, that the First Order cast too narrow a definition of what constitutes "interconnected VoIP services."[4]

(1) enable real-time, two-way voice communications;
(2) require a broadband connection from the user's location;
(3) require IP-compatible customer premises equipment; and
(4) permit users to receive calls from and terminate calls to the PSTN

However, the CALEA capability requirements were intended to apply to "…equipment, facilities, or services that provide a customer or subscriber with the ability to make, receive or direct communications…." [5] The four part test borrowed from the *E911 VoIP Order* in the *First Order*, encompasses only a small fraction of the "communications" intended to be covered under CALEA.[6] The result is inappositely narrow even when juxtaposed with the equivalency authority allowing the Commission to apply the requirements to any "...person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of [CALEA]." The need for a broader scope of VoIP and other services is discussed below.

C. Further Notice

1 Scope of Services subject to CALEA should be broadened

8. As noted above, VeriSign argues that the *First Order* casts much too narrow a "filter" regarding providers subject to CALEA. Today, the widespread deployment of Session Initiation Protocol (SIP) based services, allows a large number of providers to effectively become the equivalent of local exchange carriers that offer "services that provide a customer or subscriber with the ability to make, receive or direct

[4] *See* para. 39, *First Order*.
[5] Sec. 103(a), Communications Assistance for Law Enforcement Act of 1994, *supra*.
[6] *See* para. 39, *First Order*.

communications." [7] Indeed, the SIP protocol standard describes its use as "…an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences."[8] Providers of SIP based capabilities to the public are clearly the equivalent of exchange signaling providers within the ambit of CALEA, and will constitute a ubiquitous, service of public IP-enabled Next Generation Networks (NGN). Whether a provider interconnects with the PSTN is essentially irrelevant; and indeed as the PSTN evolves entirely into an NGN based public infrastructure over the next several years, there will no longer be interconnection with the PSTN. The SIP situ are also critical digital forensic nodes in the infrastructure that provide unique and essential communications identifying information for both law enforcement and protection of the infrastructure.

9. It is a simple and rather precise step to require that any provider of SIP-based (or equivalent) services to the public support CALEA capabilities. The capability requirements are also easily met with no impact on the technology. Indeed, standards activities toward this end are already underway, instituting innovative techniques to support worldwide requirements.[9]

2. No exemptions or alternative requirements for any classes should exist

10. Arguments that certain classes or categories of facilities-based broadband Internet access providers – notably small and rural providers and providers of broadband networks for educational and research institutions – should be exempt from digital forensic requirements under either CALEA or Title I should be rejected. To allow such exemptions would defeat the essential purpose of CALEA to provide ubiquitous digital forensic capabilities, and provide the equivalent of "safe zones" for criminals, hackers,

---

[7] *See* Rosenberg, et al., *SIP: Session Initiation Protocol*, RFC 3261, June 2002 [available at http://www.ietf.org/rfc/rfc3261.txt].

[8] Abstract, *ibid*.

[9] *See, e.g., Electronic Surveillance for Next Generation Networks*, ATIS PTSC-LAES-2005-146; *Direct Signal Reporting (DSR) for T1.IPNA*, ATIS PTSC-LAES-2005-127; *Report of the ETSI/TC LI (Lawful Interception) plenary meeting*, Sorrento, ETSI/TC LI#10, 4-6 October 2005, Doc. ETSI/TC LI (2005) 10litd054.

and terrorists to engage in unlawful activities and attack the national infrastructures. The Commission should not adopt any CALEA exemptions.

11. VeriSign and other members of the entrepreneurial and innovative global lawful interception industry have over the past several years, invested considerable money and resources in working with law enforcement and providers to develop cost-effective solutions for all providers – especially small ones. In many cases, the worldwide ubiquity of the requirements have led system vendors to "bake" flexible LI solutions into their products that can be implemented at minimal cost. [10] The only impediment to implementation domestically today principally lies in the Commission's actions in this proceeding.

12. For the same reasons discussed above, nothing less than full CALEA compliance should exist all classes or categories of providers; and would be counterproductive. Commission action in this rulemaking proceeding is not needed to provide for flexibility. The requirements are generic, and the capability specifications developed by the FBI are not based on technology platforms but on general descriptions of digital forensics if possessed by the provider. As a result, a suite of compliance standards today have been constructed with substantial flexibility to allow tailoring to specific provider platforms and implementations.[11] The desired flexibility has already been implemented by industry.

3. Ancillary capability obligations

13. The support of digital forensic capabilities should, pursuant to CALEA's Sec.103 requirements as well as Title I, include the registration of all providers to obtain an ICC/OCN, as well as the maintenance of an accessible directory of minimally authenticated users/subscribers.[12] Such registration provides the ability for law enforcement to be cognizant of providers, and to rapidly contact a responsible party and

---

[10] Subsentio, Inc., in its comments in this proceeding provided the results of an extensive analysis that indicated costs for even the smallest providers were only $0.33 additional per month for compliancy. See Comments of Subsentio, Inc., ET Docket 04-295, filed 8 November 2004.

[11] *See, e.g.*, n. 9, *supra.*

[12] ITU Carrier Codes (ICCs) - known as a Company Code (OCN) in the U.S. – are the universal basis for identifying providers. See http://www.necaservices.com/source/NECAServices_148_1606.asp. ITU-T Rec. E.115-2005, *Computerized Directory Assistance*, is an example of a secure, audited, contemporary industry standard for providing access to minimal user-subscriber directory information.

to know who is associated with a communications identifier (e.g., telephone number or IP address) being provided to enable communications. Both law enforcement and those protecting the national public telecommunication infrastructures must know this information to perform any meaningful activity.